IBM Security
Intelligence. Integration. Expertise.

IBM

Tendencias:
La madurez de los controles de Ciberseguridad en Latinoamérica.

Trends:
CyberSecurity Controls Maturity in LatinAmerica

Vicente Gozalbo Moragrega
Executive Security Advisor
WW Security Tiger Team

4 de Octubre de 2016
Miami, FL

Agenda

- Introduction
- Actual Security Activity from IBM Xforce yearly reports.
- Security Controls Maturity from the IBM WW Tiger Team.
- Key Findings.
- Actionable measures to take.

Introduction

- IBM Security Tiger Team, Executive Security Avisor means:

1. Articulate security solutions to "C-level" executives. In other words, **align security solutions to business initiatives.**
2. Tiger team members **have deep knowledge** of security solutions.
3. Act as security advocates. The tiger team act as the security-focused "**voice of the customer**".
4. **Report directly** to the IBM Security Solutions VP.

Industrias más atacadas 2014-2015 (Global).

WW Industries experiencing the highest incident Rating 2014-2015

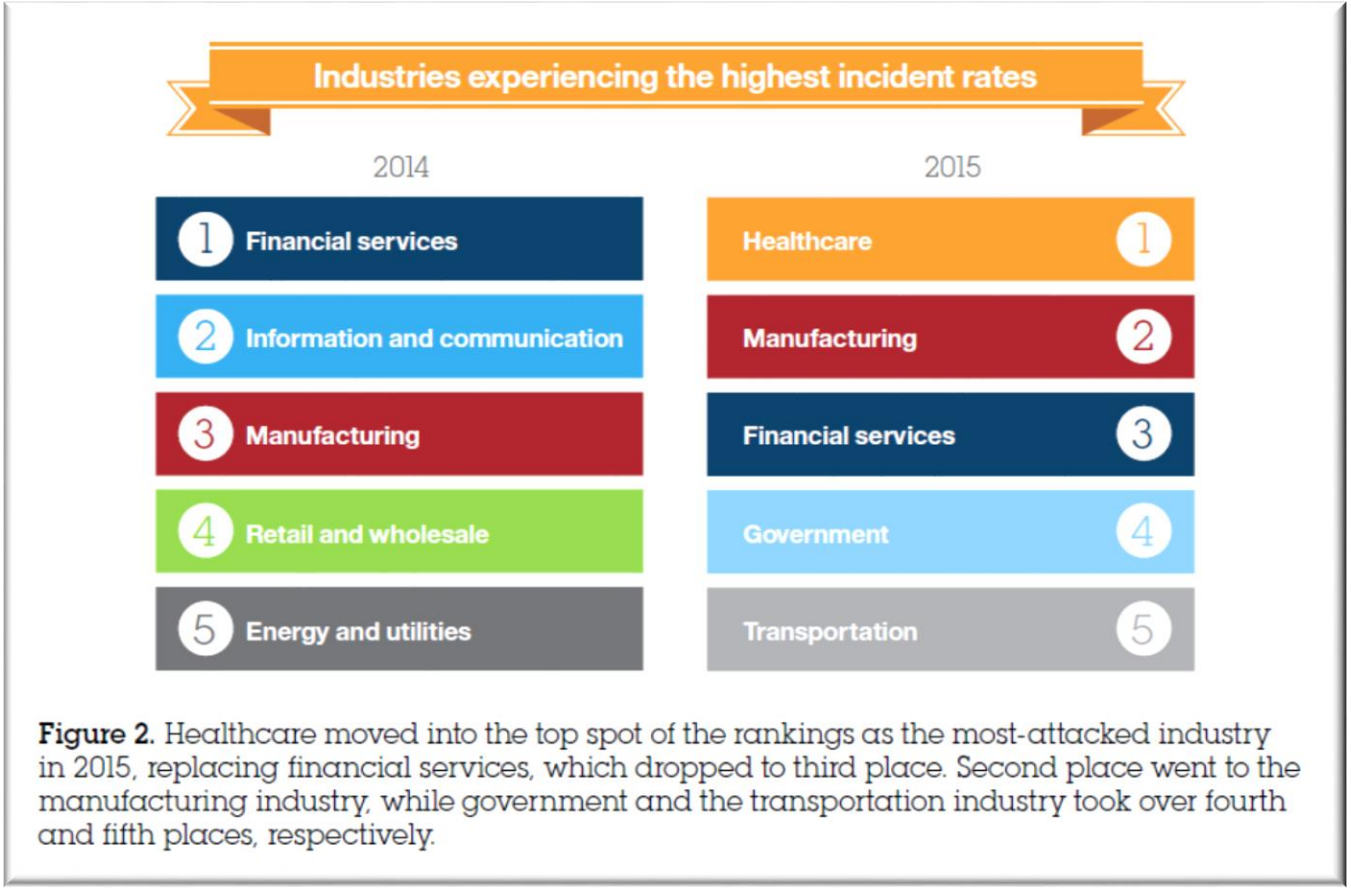


Figure 2. Healthcare moved into the top spot of the rankings as the most-attacked industry in 2015, replacing financial services, which dropped to third place. Second place went to the manufacturing industry, while government and the transportation industry took over fourth and fifth places, respectively.

Source: IBM X-Force Threat Intelligence 2016, WW Data

Incidentes más comunes en 2014-2015 (Global)

WW Most frequently incident categories

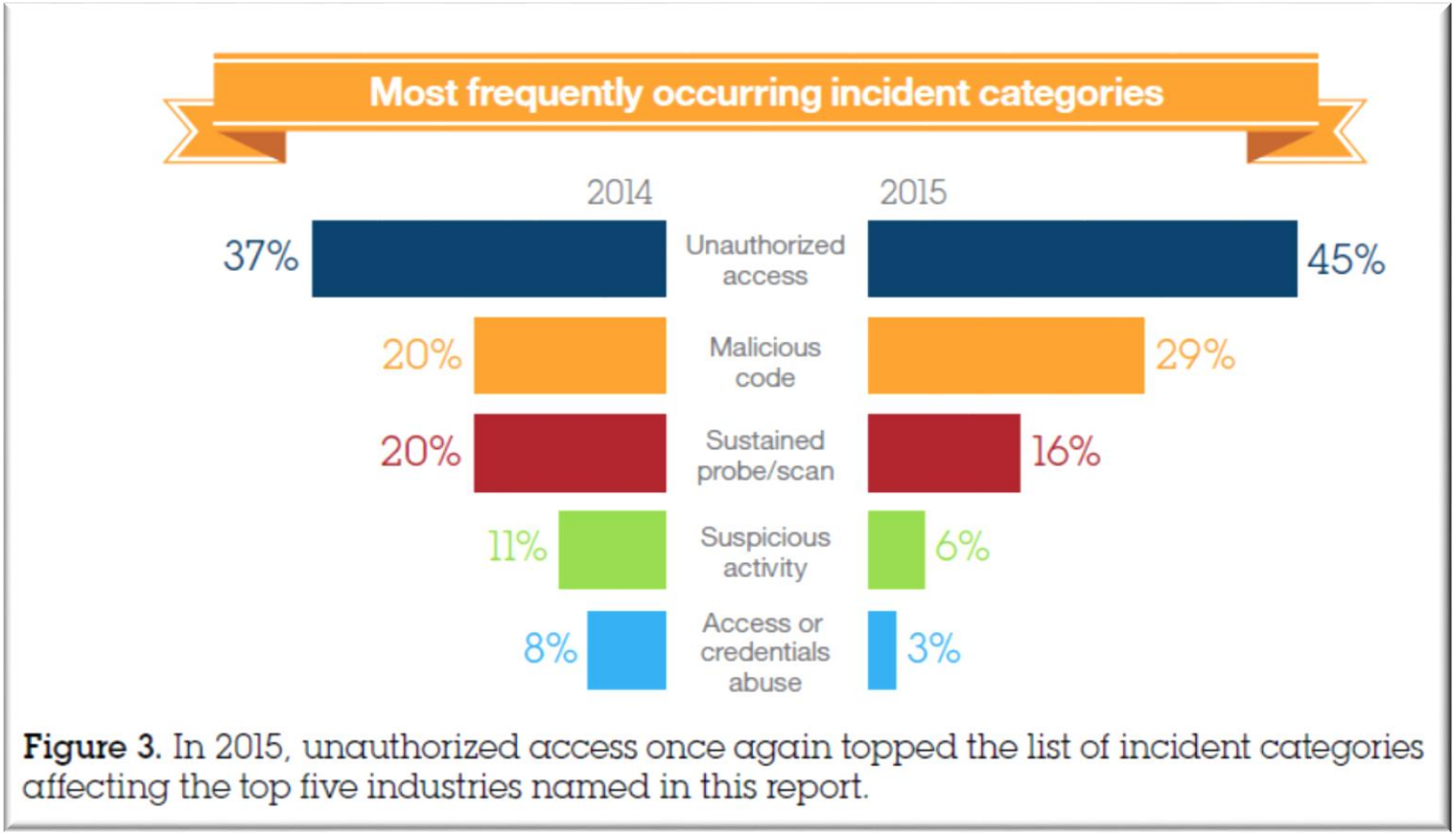


Figure 3. In 2015, unauthorized access once again topped the list of incident categories affecting the top five industries named in this report.

Source: IBM X-Force Threat Intelligence 2016, WW Data.

Panorama de la Ciberseguridad desde las Organizaciones
Madurez de la Seguridad

CyberSecurity Landscape from Organization's Security Maturity

Taller de Madurez de la Seguridad Corporativa

Enterprise Security Maturity Workshop

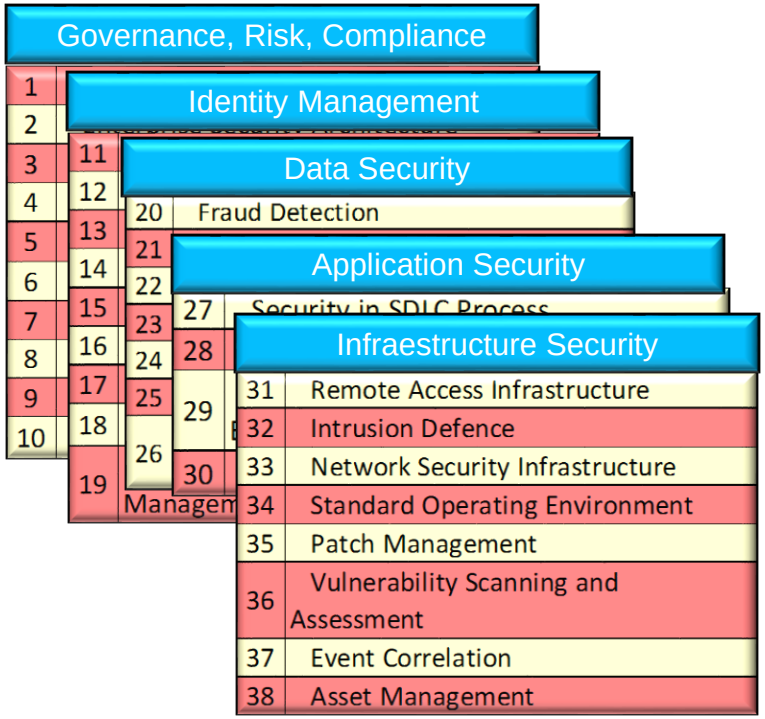
Each Workshop
38 Security Controls
ISO 27K
COBIT
Benchmarking
+300 hours

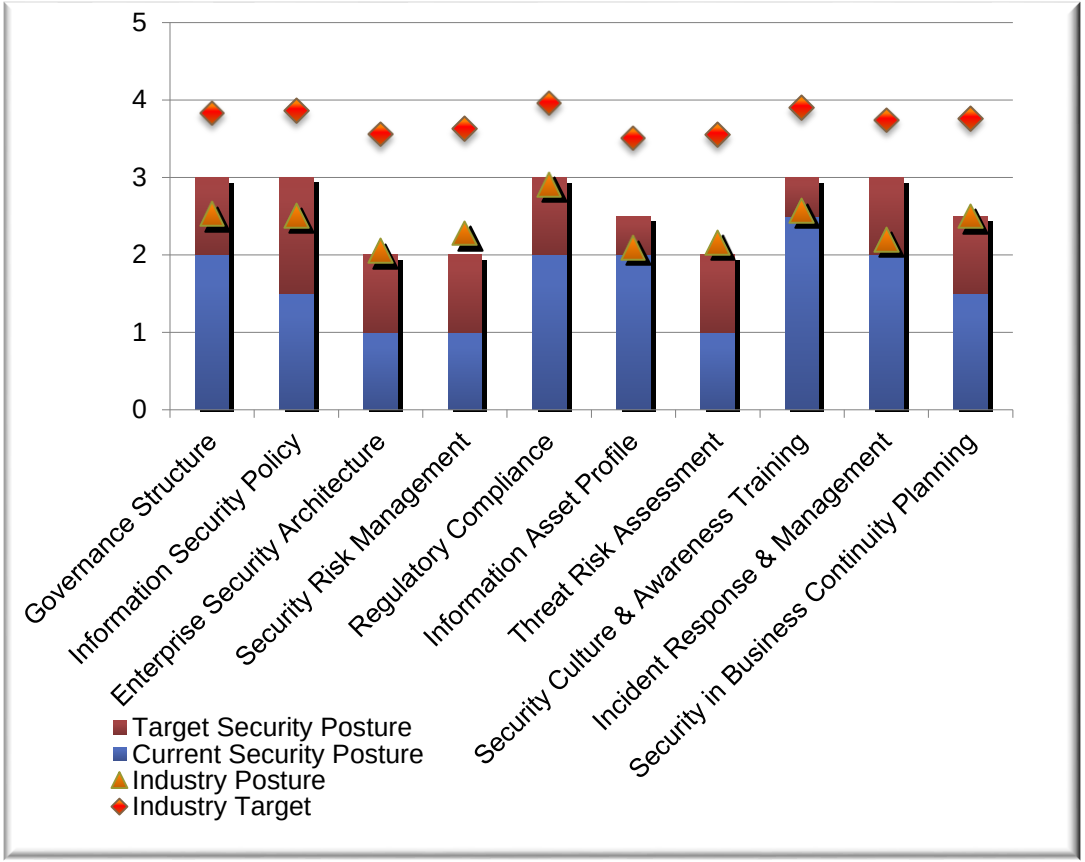
- Revisión de 38 controles de seguridad ISO 27K, mediante meotodología COBIT.
  - *Subset of 38 ISO27K Security controls maturity review, COBIT Method*
- Madurez autoevaluada de 1 (Inicial) a 5 (Optimizada), guiada por experto de IBM
  - *IBM expert guided self assestment 1 (initia) to 5 (Optimizing), for each control.*
- Benchmarking según industria.
  - *Industry (Financial) Benchmark*
- Análisis cuantitativo y cualitativo de la Posición actual de seguridad, posición futura
  - *Qualitative and Quantitative analisys to depict current and target Security maturity posture.*
- Más de 300 horas repartidas en / hours
  - 5 Teleconferencias / *Teleconferences*
  - 1 día completo de discusiones / *complete discussions day*
  - 1 presentación ejecutiva de resultados / *Executive result presentation*

Enterprise Security Maturity Workshop:

38 Controles de Seguridad ISO 27K evaluados con un modelo COBIT de madurez.

38 ISO 27K Security Controls assestment with COBIT Model to get current tand target Security Posture





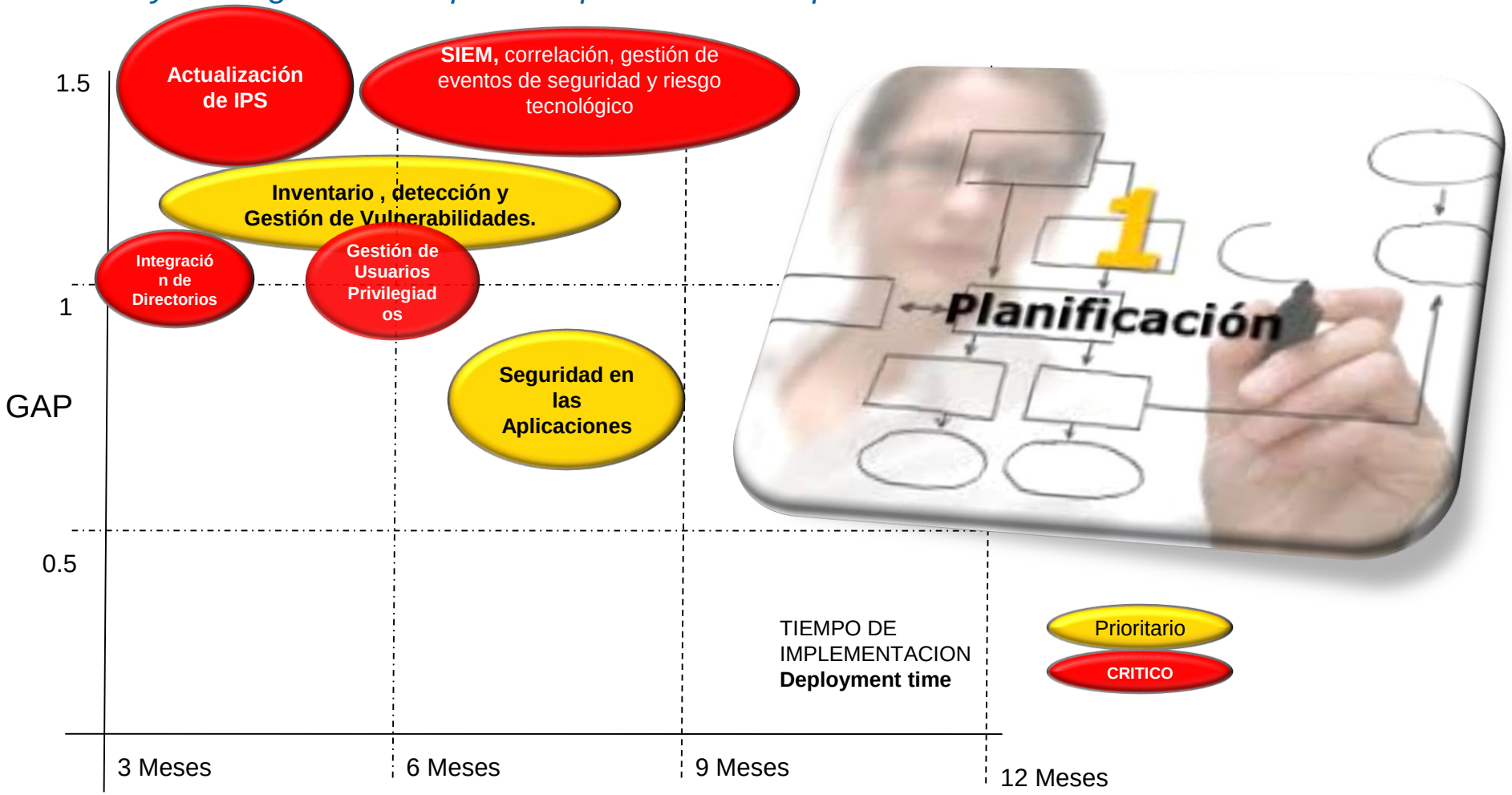
Panorama táctico: Controles con más GAP

Tactical Landscape: Controls with more GAP

Domain	Control	Current Maturity	Gap	Target Maturity
Infrastructure	Intrusion Defence and Protection	2.5	1.5	4
People	Identity Establishment	4	1	5
Application	Application Inventory	2	1	3
People	Persons Identity Lifecycle Management	2.5	1	3.5
People	System and Service Account Lifecycle Mgmt	2	1	3
GRC	Regulatory Compliance	3	1	4
Data	Fraud Prevention & Detection	2	1	3
People	Remote Access To Corporate Data and Apps	2	1	3
People	Privileged & Shared Identity Management	2	1	3
Data	Data Classification & Database Configuration	2	0.5	2.5
Infrastructure	Asset Management	2	0.5	2.5
Infrastructure	Vulnerability Scanning & Assessment	2.5	0.5	3
Data	Data Transaction Security	2	0.5	2.5
Application	Secure Design & Threat Modelling	2.5	0.5	3
GRC	Information Security Policy	2.5	0.5	3
Data	Data Lifecycle Management	2	0.5	2.5
Infrastructure	Patch Management	2.5	0.5	3
Application	Secure Coding Practices	3	0.5	3.5
GRC	Security Risk Management	2.5	0.5	3
GRC	Incident Response & Management	2	0.5	2.5
GRC	Security in Business Continuity Planning	2	0.5	2.5
Infrastructure	Network Security Infrastructure	2	0.5	2.5
People	Authentication Services & SSO	2	0.5	2.5
Application	Application Security Assessment & Testing	2.5	0.5	3
GRC	Security Culture & Awareness Training	2	0.5	2.5
Application	Vulnerability Remediation & Risk Mitigation	3	0.5	3.5
GRC	Enterprise Security Architecture	2	0.5	2.5
Infrastructure	Event Correlation	2	0	2
GRC	Governance Structure	3	0	3
Infrastructure	Standard Operating Environment	2.5	0	2.5
GRC	Information Asset Profile	2	0	2
GRC	Threat Risk Assessment	3.5	0	3.5
Data	Encryption & Key Management	2	0	2
People	Authorization Services	2.5	0	2.5

Panarama estratégico de seguridad – Hoja de ruta

Security Strategic Landscape – Proposed Roadmap



Madurez de los controles de Seguridad en Latino América. Visión desde el WW STT - LA

Security Controls Maturity in LatinAmerica. Vision from the IBM WW STT - LA

ESMW Execution

+150 clients WW

16 LA customers
10 LA Countries

+350 LA Security & LoB experts

- Realizado en más de 150 clientes seleccionados en todo el mundo de todos los sectores.
  - Carried out for + 150 countries World Wide, all sectors
- En Latinoamérica se ha ejecutado en 16 clientes del sector financiero de 10 países.
  - México, Guatemala, Costa Rica, Panamá, Colombia, Perú, Ecuador, Venezuela, Chile, Bolivia
- Auto-Evaluaciones recibidas de más de 350 especialistas del sector **financiero**.
  - Guided Self assestment done from more tan 320 security and LoB specialist from finncial industry in LA.

Estadísticas Comparativas
Comparative Statistics

5 Mejores controles – Media / *5 best controls - Average*

Domain	Control	Current Maturity	Gap	Target Maturity
GRC	Regulatory Compliance	4	1	5.00
People	Identity Credential Management	3.1	1.3	4.40
GRC	Security Culture & Awareness Training	3	1.5	4.50
GRC	Information Security Policy	2.75	1.09	3.84
Application	Application Security Assessment & Testing	2.74	1.37	4.11

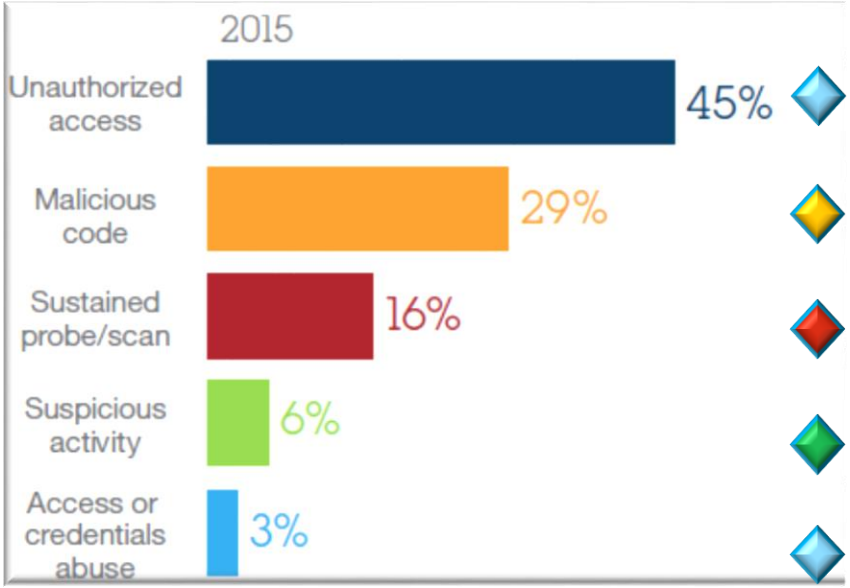
Estadísticas Comparativas
Comparative Statistics

5 Peores controles – Media / *5 worst controls - average*

Domain	Control	Current Maturity	Gap	Target Maturity
People	System and Service Account Lifecycle Mgmt	1.8	2	3.80
Infrastructure	Event Correlation	1.8	2.4	4.20
Infrastructure	Asset Management	1.76	2.72	4.48
People	Privileged & Shared Identity Management	1.75	2.65	4.40
GRC	Information Asset Profile	1.5	1.75	3.25

¿Hay alguna relación?
There is any relationship ?

Domain	Control
People	System and Service Account Lifecycle Mgmt
Infrastructure	Event Correlation
Infrastructure	Asset Management
People	Privileged & Shared Identity Management
GRC	Information Asset Profile



Causa Raíz
Root Cause

Análisis Cualitativo. Preocupaciones en la CyberSeguridad.

Qualitative Analisys. Worries in Cybersecurity

- Internet de las Cosas: Miles de millones de dispositivos vulnerables interconectados

  Internet Of Things: billions of vulnerable devices interconnected

  – Los índices de Cyberseguridad y Madurez no van a mejorar

  – *Maturity measures will not get better.*

- Carencia en Formación de profesionales:

  Lack of Security Skills

  – Toma mucho tiempo en formar a personal civil o militar en tecnologías de seguridad

  – La complejidad es tan amplia que no existen “generalistas”

- Redes Sociales

  Social Networks

  – Más de un cuarto de la la Humanidad volcando información sensible que puede ser usada por terroristas, activistas, inteligencia extranjera…

    • *More than one quarter of the world population uploading personal and sensitive information ready to be used by terrorists, activist, foreign intelligence services… scaring*

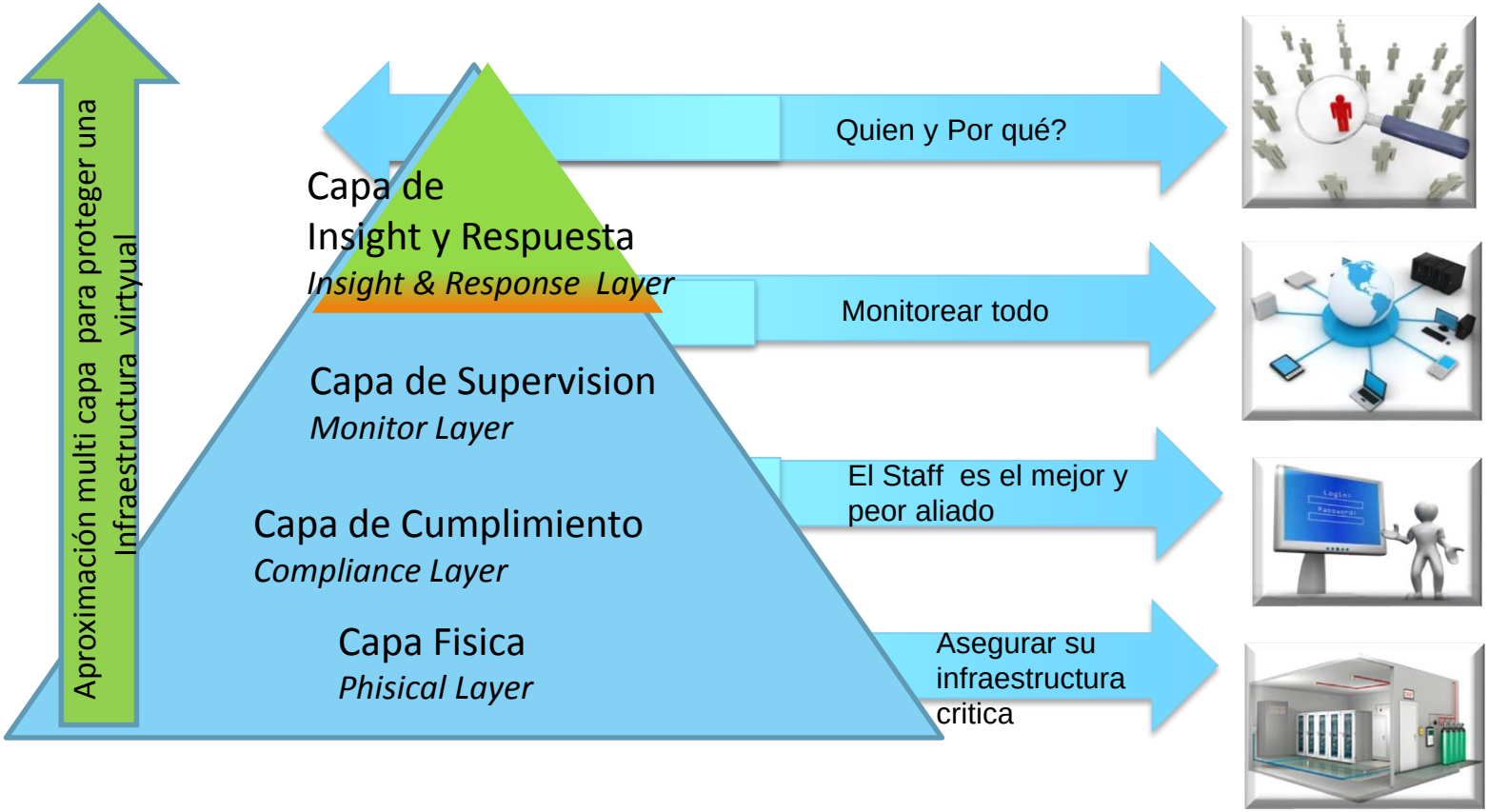
  – Suplantación de Identidades en todas sus formas.

    • *Identitity Theft in all their possibilities*

SIGUIENTE GENERACION DE SOCs / *Next SOC Generation*

La Siguiente Generacion de SOC necesita tener foco en todos los niveles

Next SOC generation will need focus in all the layers



Medidas factibles a tomar

Actionable Measures to take

Medidas a tomar
Urgent measures to take

#1 : Asset Management and Security Information Classification

- Necesita aplicar tecnología para mantenerlos actaulizados en tiempo real
  - You will need to apply technology in order to keep inventories updated to real time
- Foco: BYOD, MDM. Piense en soluciones SaaS. Rápidas y de bajo riesgo en implementación
  - Focus on BYOD And MDM. Think in SaaS Solutions: Fast and low risk in implementations
- Sin excepción: Cualquier dispositivo que se conecte a la infraestructura corporativa debe estar inventariado.
  - No exception: Any device connectig to corporate information infrastructure should be managed.

Fiberlink Maas360, Big Fix

Medidas a tomar
Urgent measures to take

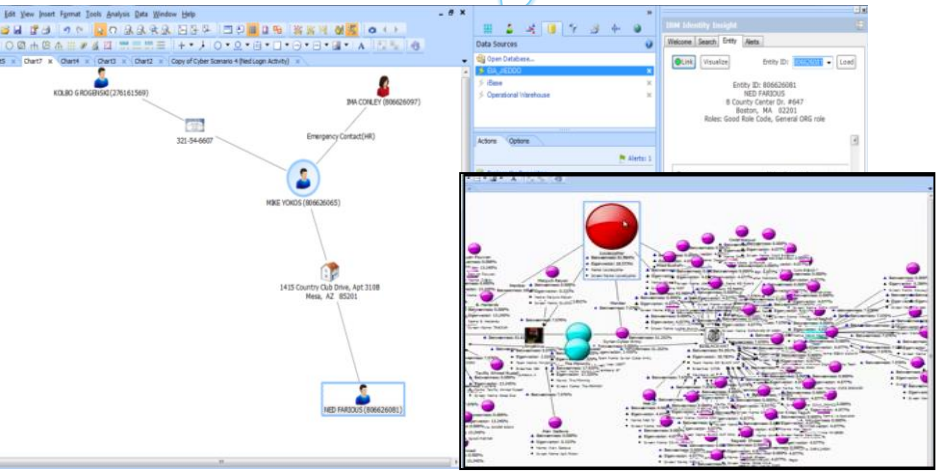
#2 Privileged, shared and service credentials lockdown

- Establecer controles para el uso de cuentas privilegiadas. Apoyarse en tecnología
  - *Set specific controls for privileged account credentials. Relay on technology.*
- El Acceso privilegiado no autorizado es el riesgo tecnológico más importante para el negocio.
  - *Unathorized privileged Access is the most important technlogy risk for the business*
- Grabar en formato de video toda actividad
  - *Video recording all privileged activity*

Privileged Identity Management

Medidas a tomar
Urgent measures to take

#3 Apply Advanced Analitycs



I2 Enterprise Insight Analisys

- Hallar relaciones y anomalías en grandes cantidades de data, para ayudar en investigación.
  - Find relationships and anomalies in huge amount of data in order to help reduce time in investigations
- Diferenciar entre operaciones normales y anormales rápidamente
  - Rapidly Differentiate between normal and abnormal operations
- Conectar los puntos e Identificar patrones y Concentraciones de Actividad.
  - Connect the dots and identify schemas and activity hubs
- Identificar los Actores de la amenaza Y los Vectores de amenaza en tiempo real
  - Real time detection vector and thread actors

Medidas a tomar
Urgent measures to take

#4

Start Cognitive Security and Incident response Projects

IBM Watson for Security and IBM Resillience

- Mejore a sus consultores de seguridad con Inteligencia Artificial
  - *Enhance your Security Analists with Artificial Intelligence*
- Acelere la respuesta ante incidentes con con inteligencia externa
  - *Speed Incident response with external intelligence and advanced software.*
- Refuerze la seguridad de las aplicaciones, son el proceso del negocio
  - Strengenth Application Security, they are the business core process

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.